

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2 Криптоаналіз шифру Віженера. Варіант — 1

Виконав:

студент III курсу ФТІ

групи ФБ-95

Чорний Анатолій

Перевірила:

Селюх П. В.

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

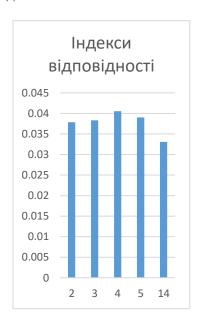
- 0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- 1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r=2,3,4,5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
- 2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
- 3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

В якості тексту для шифрування був взятий уривок роману «Фауст» Гётте. Труднощі виникли на етапі отримання ключа, де осмисленність ключа псувалась однією літерю. Проблема була вирішена за допомогою автоматизованої підстановки наступних за популярністю літер алфавіту у формулу $k = (y^* - x^*) \mod m$,

Обчислені значення індексів відповідності для вказаних значень довжини ключа:

Довжина ключа	ключ	Індекс відповідності		
2	да	0.03785816305710205		
3	кот	0.038340086085444175		
4	маша	0.04054954771135143		
5	толик	0.03901827615355467		
14	япишулабуночью	0.033089456962136006		



Набори значень індексів відповідності, одержаних при встановленні довжини ключа

			-			
2	3	4	5	6	7	8
0.034329214	0.037348391	0.038467868	0.032753685	0.042422498	0.032845672	0.038394305
9	10	11	12	13	14	15
0.037406913	0.034343107	0.03282596	0.054369557	0.032807635	0.034253133	0.037414411
17	18	19	20	21	22	23
0.032607688	0.04261924	0.032998523	0.038394078	0.037345969	0.034363464	0.032488237
24	25	26	27	28	29	30
0.054354166	0.032517536	0.034348577	0.037625003	0.038386039	0.033132184	0.042504501
31	32					
0.032704275	0.038534413					



Зашифрований текст:

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрм увнусьъюоыюдежжьсбххиуьнпеуссдкруытчкбзхсаьмгяшквецфяылхсйювукзпефшфйармжйачыэшю мтэдвзухщбиэтэюврыучшпуютерпэбьпвбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацф яюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгфьробфбрикаычсяэтэзшшпкачъроэюп вщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлькщярфбйхпзиеиюэхроыьуэютпзк мгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжс тээуэйттфрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежизыиэтюгчвипкачъроэроккечшэкшлбьяп ьшчсснацщибзбмкхфуюошвноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбь фюхоштзънцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшсвецфщищтйдвнме шьиюнаэххсзичптфчапдвнтеуодшчюлуэднжфчиздтибфюфшршюиибжфррффдчсьъюоыюузийтюпх фдбэжвгутхяыуйшркремшхэйаььснидечэкчюмууяздийюпьхвтрвжэпкачьроягевбчпвлмафъмюгжыц сьиэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщкухщсгэбяьд ъшкьцэъясуткббчивлкъбсвъдайтгфавигьивяанбиубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбы гжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыф юмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаараричэтэюьбарюсжсчпжъюошвмкв уняждищэгивщахсргьошфитжлиээнщтбсрфъкчюэстиетъужзигьрънбидфзуыяснвфшвдукнящофгу ыеноахтглипубугвдатюфмюугюмздийхэшэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжг эщьбщисзйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрруг шбщбщпвшфяябхптоъррбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбю юнжеефямъюуяркэбспюоывжлшкреуьлокыжаэъльныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжчч цвъюошвнижхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгша ддвшчсзрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгучжа экхишэмэдсеаяиябюшвремкьэыепчисгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйшхм кюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщииумжияакнлдя жилуязфитыычсбгыбсрвзишсиръуосучиптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюц фжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвищбэты аелиежххсьххишбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяисперифэчшфуиббяшяпкуч щэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцьоууквччевщцвйарвремкьэцэубгепэф шгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчя фвтэглтрлцынфвшляъьыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуьыяг впшьнтэфъяждюуфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженж ччляефроахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуцыд флсюидояыщэйяшрэщеыглээахчаэркчсььюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквхррэцхщр ывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрзду ърчцъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтижхрачртывдфжтпэбцэжяяпрсеугфохо ушгзкнлбпъясбйялкучцыъюошьсрекцсьъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбюютчжййг тиэиуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржб сррнссяцбщищбзикыыэфшмыфпрвуцхпщтжгизфйдмяьзупдянжедчясщхууьзбщащбфмяпкхкхдкъцб дбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчш укцвжйьнлднхмищтпшобницьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуынуфььятцаа мрюудухсюцвпэрлкйчъдчъбадэдгжимяуиэпхюкпуйшвбрубхиззеклиащсйхрккзркэоцъбэпрфиеосъибугр гвебйаэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчу бахйдсузыцямжжжьдичммджрвйитнсгбэукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяызьпгхбдэхн ьпйлгъхлпукчиушртэюпзбьпэюцумбвзффкидуиыбфлйриельлшэждзяуктеэчуоепьзсиуыафшюфехчюй дщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбцэжв юрфиеосъзттигрфиутьциспепрюжчптффюжчисбжйшифишжчимукзпюьцимссзожомцудвьах жпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзццтжебюсиуыафшюйквнздшщбчхреюхекк шлятиприйдтистбпхфбгррузхкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжб

вйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжв оцвсыьзтштосаухиобнукхкхихмадвннфжихаътжаэнзвуьсрухлггчзебпыэъюсбхнсгефщсихщивъбйнхя нрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшав гзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпк лшубсрйулщяиыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвю напаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцю гвачеюпкхсаюдпэсшчфамгдяноеньнэьюнквнгуршаянцешьзтштосьнвавюлпцфъяачхсбвъсжсчщздзуб иджжстьчуоешщоръкосшиспхбдопчивээабашквкамапфпуыббрэощяокыашврбекмщурьььрпкхржяь чюжетррзхиуэофжашзолмеычпроыьрнэйэцбьхсчимвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпр ъуодбрембьнтэзхиттюквыюувкыаънблбьпхвишэщхшушъпхысчиушгзаюбфжхйуьрьбьвджлътвэкбж ибсриучфпыубжрпкхржаагбубаниэзецьищушфтчаикдтигбгшьнфзчщыищушьнтэццяьтыпчркюкня саулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыьпю ъквкумцяхюдыьмэяйпйьрьвбидукзкэощьжгвыркыкяюурлытябыуънщибйчхкпшжпбфлггчатезумяъхр нэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэ кшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэ тфацьсьнврююсюэишафщъпяънтирхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщури спуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшр отвдежфивънфоышррешпбурэбафорэчырсчхтахножкиябюхошьнелчлмбдчжяэъоавьщикглыюмкйг осьрбибфюфйзевэьлргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвн жльштэохлуьнпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбз юоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуф нгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътя ншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрс эхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбсни лщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеан дэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхс еэябдньсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчьмеупвърсафлкфшснхф люгбаюфеечцызсьюсъкязыцдтвпиюбриньюпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфв гчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэж уяннчдысыфюйцыяйшцьидчюсахотжцежпушлуъбкькхщжьюнбщнфэыфяяцыэвювкщзцяящъйитнне еяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбс зйцеюэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцьножихщргюргюбзиичдбдхьш эддикцрачхсхюврюкмитупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцф бятрнльщяаугщущсзйнчнэшчбкхлсжмшбчьхтшсюпэфъссмюк

Ключ:

вшебспирбуря -> вшекспирбуря

Розшифрований текст:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланск ийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеапол итанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныека либанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросы мирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепр оспероместодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляиб оцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналет имнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселе йживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешь входяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянате

бяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцма навамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещев ыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетд еладокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянаборту боцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможет посоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувлас тьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовь тесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуход ятгонзалооднакоэтотмалыйменяутешилонотьявленныйвисельникакомусужденобытьповешенным тотнеутонетофортунадайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговер евкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешен ныммыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстеньгуживониженижепопроб уемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсв истоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавас иидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезж алостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоим сяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкораб льбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойба быбоцмандержикручекветрукручеставьгротифокдерживоткрытоеморепрочьотберегавбегаютпр омокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкор митьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантон ионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонза лонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрико рабляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемр ядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплод нойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакия быпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимиранда мирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалос *ьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястр* адаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдира збилсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомямореввергл абывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипроспероутешьсяпу стьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперониктонепострад алявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиотку дачтоведомотебечтотвойотецзоветсяпроспероичтоемупринадлежитубогаяпещерамирандарассп рашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойпла *щволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьяст* ольбедственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсе осталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволосне упалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисво йрассказсловаминетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепосели лисьмытебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемира нданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятис воейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпое тдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновтор явнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмо лклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонау молклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолна мкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменя

влечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанет плотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплошенчуслышен похоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинан дпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпросперомиран деприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьот еипрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткак мыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьвра гкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназва ланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэль искусныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотги мнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавн ыйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофердинандка кмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросп еропервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнил пронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотеикорольпогибв морскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгери огвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутье шеневремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодам вслухпослушайтесиньорзачемпозоритесебянеправдой

Висновки: в ході виконання компьютерного практикуму мною були дослідженні методи розшифрування тексту зашифрованного шифром Віженера. Також було обрано один із методів и відвтворенно на мові програмування руthon. У ході розшифрування був використан метод співставлення індексів відповідності для відтворення довжини ключа, та розшифрування серії шифртекстів закодованних шифром цезаря, за допомогою частотного аналізу.